RESEARCH AND DEVELOPMENT

RECOMMENDATIONS FOR PROTECTING AND ASSURING CRITICAL NATIONAL INFRASTRUCTURES

Report of the
President’s Commission
on Critical Infrastructure Protection

1997

ACKNOWLEDGMENTS

Many individuals at the Commission and within government, the Department of Energy national laboratory system, academia, and the private sector made important contributions to this report. In particular, the Commission gratefully acknowledges the assistance provided by Commissioners John Davis, David Jones and Merritt Adams; and James Peerenboom and Thomas Wolsko from Argonne National Laboratory, as well as the many valuable contributions made by the Commission's Laboratory Council and the research and development strategy teams from the Department of Energy's national laboratories. We also thank Blaine Burnham of the National Security Agency for characterizing information security research in the Department of Defense and Intelligence Community, William (Terry) Mayfield of the Institute for Defense Analyses for assessing commercial information assurance research and development, and Anita Jones of the University of Virginia for providing insightful review comments. Finally, we thank Carol Medill, Commission staff analyst, for providing valuable administrative assistance.

Members of the Commission's Laboratory Council
Terry Surles and Paula Scalingi, Argonne National Laboratory
Robert A. Bari, Brookhaven National Laboratory
David F. Cauffman, Idaho National Engineering Laboratory
Stewart Loken, Lawrence Berkeley National Laboratory
Ronald W. Cochran, Lawrence Livermore National Laboratory
Houston Terry Hawkins, Los Alamos National Laboratory
David E. Reichle, Oak Ridge National Laboratory
Landis D. Kannberg, Pacific Northwest National Laboratory
Samuel Varnado, Sandia National Laboratory

Leaders of the DOE National Laboratory R&D Strategy Teams
Ron Fisher and Dorland Edgar, Argonne National Laboratory (Oil & Gas)
James Peerenboom, Argonne National Laboratory (Interdependencies)
Tom Wolsko, Argonne National Laboratory (Electric Power Systems)
Trevor Pratt, Brookhaven National Laboratory (Interdependencies)
William Johnston, Lawrence Berkeley National Laboratory (Information & Communications)
Kathleen Bailey, Lawrence Livermore National Laboratory (Information & Communications)
Doug Mansur, Lawrence Livermore National Laboratory (Information & Communications)
Bill Hunteman, Los Alamos National Laboratory (Information & Communications)
Darryl Morgeson, Los Alamos National Laboratory (Transportation)
Mike Bronzini, Oak Ridge National Laboratory (Transportation)
John H. Sorensen, Oak Ridge National Laboratory (Emergency Services)
Bernie Saffell, Pacific Northwest National Laboratory (Oil & Gas)
Lance W. Vail, Pacific Northwest National Laboratory (Water)
Samuel Varnado, Sandia National Laboratory Albuquerque (Banking & Finance)

CONTENTS

TABLES

FIGURES

Executive Summary

RESEARCH AND DEVELOPMENT
Recommendations for Protecting and Assuring Critical National Infrastructures

This report summarizes research and development (R&D) recommendations for the President's Commission on Critical Infrastructure Protection (PCCIP). These recommendations address the eight critical infrastructures[1] identified in Executive Order 13010 as well as crosscutting, interdependency issues that affect more than one infrastructure.

The goal of the R&D recommendations is to provide a roadmap for the development of technologies that will counter threats and reduce vulnerabilities in those areas having the potential for causing "significant" national security, economic, and/or social impacts. Specific technologies considered are those that protect infrastructure and thereby reduce vulnerability; detect intrusions and provide warning; mitigate the effects of disruptions (incidents); assist in the response management of incidents; and facilitate recovery.

Basic research requiring long-term government investment is emphasized. This research must be accompanied by *technology development* within the private sector. Technology, broadly defined, includes processes, systems, models and simulations, hardware, and software. It is essential to have strong involvement from infrastructure owners and operators to ensure the development and acquisition of useful and usable products.

[1] Information and communications (telecommunications), electric power systems, gas and oil delivery and storage systems, banking and finance, transportation, water supply systems, emergency services, and government services.

Summary of R&D Recommendations

1. *Conduct research and development in six areas:*
   * *Information assurance*
   * *Monitoring and threat detection*
   * *Vulnerability assessment and systems analysis*
   * *Risk management and decision support*
   * *Protection and mitigation*
   * *Incident response and recovery*

2. *Increase the federal investment in infrastructure assurance research to $500 million in FY99 and incrementally increase the investment over a five-year period to $1 billion in FY04*

3. *Establish a focal point for national infrastructure assurance R&D efforts and build a public/private-sector partnership to foster technology development and technology transfer.*

The six recommended areas are:

- **Information Assurance**. Significant new investment and effort in R&D are required for effective protection of the communications infrastructure, and the information created, stored, processed, and transmitted on it. Assurance of vital information is increasingly a key component to the functioning of our interdependent infrastructures. The urgent need to develop new affordable means of protection is apparent, given the increasing rate of incidents, the expanding list of known vulnerabilities, and the inadequate set of solutions available. This sense of urgency is further compelled by the increasing rate of system integration and the resulting complexity of those infrastructure information systems whose behavior is becoming much less predictable.

- **Monitoring and Threat Detection**. Reliable automated monitoring and detection systems, timely and effective information collection technologies, and efficient data reduction and analysis tools are needed for identifying and characterizing localized or coordinated large-scale attacks against infrastructure (National Cyber Defense). Such technologies would support early threat warning to government organizations and private-sector infrastructure owners and operators, thereby preventing widespread infrastructure disruptions that have potentially serious consequences to our national security, economy, and quality of life

	• **Vulnerability Assessment and Systems Analysis**. Advanced methods and tools for vulnerability assessment and systems analysis are needed to identify critical nodes within infrastructures, to examine infrastructure interdependencies, and to help understand the behavior of complex systems. Such methods and tools would allow issues, such as physical and cyber security, to be addressed in an integrated fashion. Modeling and simulation tools and test beds for studying infrastructure-related problems also are important for experimentation that cannot be performed in realistic environments of any appreciable scale. In addition, techniques to verify and validate methodologies and tools are needed. • **Risk Management and Decision Support**. Risk management and decision support system methodologies and tools are needed to help government and private-sector decision makers effectively prioritize the use of finite resources to reduce risk. These methodologies and tools would address risk from both familiar threats (e.g., natural disasters, physical attacks) and emerging and future threats (e.g., risk that arises from our increasing interdependence and reliance on cyber systems). • **Protection and Mitigation**. Real-time system control, infrastructure hardening, and containment and isolation technologies are needed to protect infrastructure systems against the entire threat spectrum. Other advanced survivability, reliability, or assurance enhancement measures also need to be explored and/or developed. • **Incident Response and Recovery**. A wide range of new technologies and tools are needed for effectively planning for, responding to, and recovering from incidents, such as natural disasters and physical and cyber-based attacks that affect local or national infrastructures.

We Recommend:	A government investment on the order of $500 million in FY99, gradually increasing over a five-year period to about $1 billion in FY04, is needed to address these infrastructure assurance research needs. This increase, an approximate doubling of investment in FY99, is needed to “jump start” a focused, coordinated, and goal-oriented national research effort. In addition to this government investment, a similar or greater level of commitment and technology development investment is needed from the private sector. This increase in investment should occur as market demand for infrastructure assurance technology increases.

We Recommend:	Close coordination and an innovative partnership among government, industry, and academia are essential for a successful research and technology development effort. To facilitate a joint effort and to ensure efficient use of limited R&D funds, a focal point (coordinating entity) for national infrastructure assurance R&D efforts is needed. Accordingly, the Commission has proposed that the National Infrastructure Assurance Office be established to stress partnership between government and the private sector, coordinate with established advisory and information exchange groups, and promote awareness and education. Its missions would include developing, coordinating, prioritizing, and overseeing the R&D agenda to meet critical national needs. It also would serve as a clearinghouse for disseminating such information. Appropriate government agencies should manage federal infrastructure-specific R&D efforts.

We Recommend:	The National Research Council define more fully a national infrastructure assurance research program based on the information contained in this report. The Council should be designated to lead the effort, together with those departments and agencies of the federal government already engaged in R&D relevant to each infrastructure.

1. INTRODUCTION

> Our nation's infrastructures are undergoing a profound change. Networked information systems are becoming critical to the daily operation of increasingly large segments of government, industry, and commerce. Moreover, in responding to the needs of subscribers, critical infrastructures like the electric power utilities and public switched telephone network are increasing their dependence on computers and communications networks. But this growing dependence on networked computers is accompanied by increased risk. First, the infrastructure becomes vulnerable to new forms of attack—attacks that may not require physical penetration of a specific site or system by the perpetrator—and the number of targets is increased. Second, the use of extremely complex technologies always presents risks. For example, software systems today are rarely free of defects and are notoriously difficult to configure and operate. Finally, the interconnection of previously isolated infrastructures enables the propagation of attacks and failures from one to the other. In short, our nation's infrastructures could well evolve into an interdependent system of fragile and vulnerable subsystems. Understanding how to ensure that they will operate reliably is thus vital. [1]

Assuring reliable operation of critical national infrastructures requires a multifaceted, harmonized strategy. Such a strategy will include research and development (R&D), education and awareness, training, policies and standards, streamlined regulations, investment incentives, and other elements that involve both government and the private sector. This report focuses on R&D as one of these important elements.

1.1 PURPOSE AND SCOPE

This report summarizes the R&D recommendations of the President's Commission on Critical Infrastructure Protection (PCCIP) in support of its mission to develop an overall strategy for protecting and assuring the continued operation of the nation's critical infrastructures. The recommendations address the eight critical infrastructures identified in Executive Order 13010: information and communications (telecommunications), electric power systems, gas and oil delivery and storage systems, banking and finance, transportation, water supply systems, emergency services, and government services. They also address crosscutting, interdependency issues that affect more than one infrastructure. Near-term (< 5 year timeframe) R&D activities are emphasized, although long-term needs are addressed in selected areas.

The goal in making these recommendations is to support the development of technologies that will address the threats to, and vulnerabilities of, critical infrastructures that have potential for causing "significant" national security, economic, and/or social impacts. As illustrated in Figure 1.1, the technologies considered are those that:

- Protect infrastructure and detect intrusions,
- Mitigate the effects of disruptions (incidents),

- Assist in the management of incidents, or
- Facilitate recovery.

Basic research requiring long-term government investment is emphasized. This research must be accompanied by technology development within the private sector. Technology, broadly defined, includes processes, systems, models and simulations, hardware, and software. It is essential to have strong involvement from infrastructure owners and operators to ensure the development of useful and usable products.

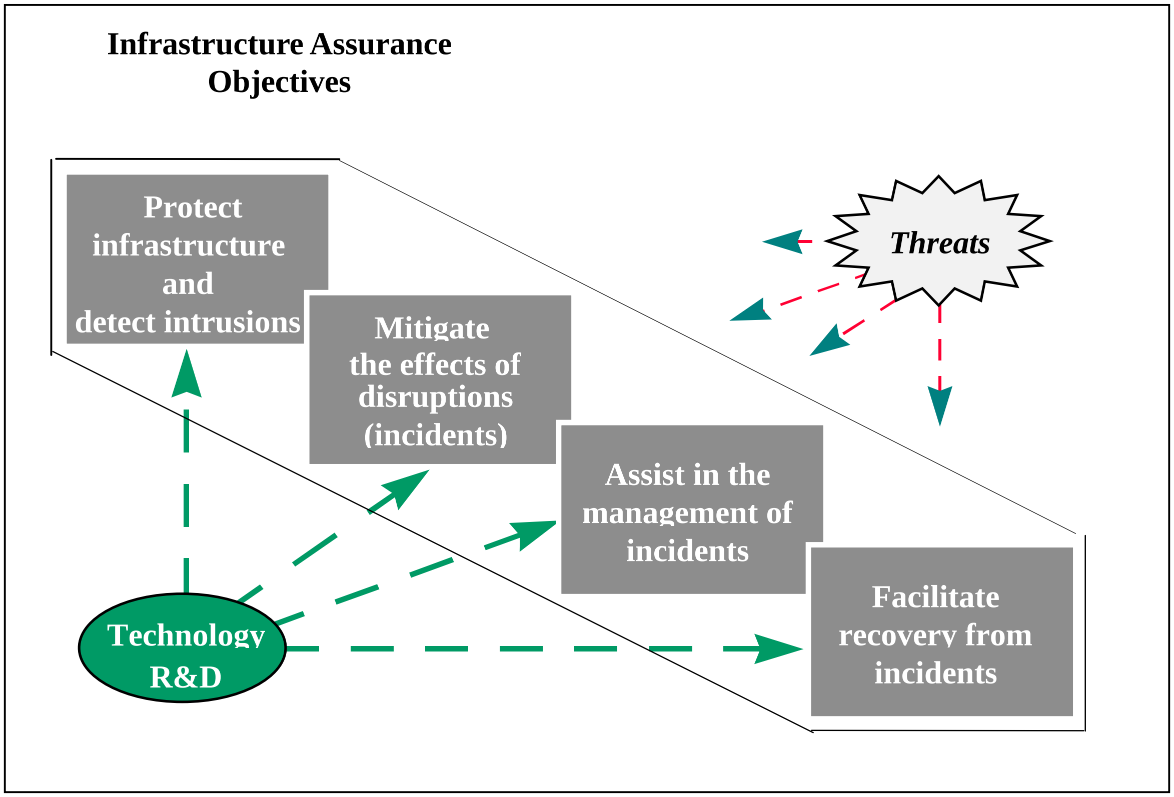
Infrastructure Assurance Objectives
Protect infrastructure and detect intrusions
Mitigate the effects of disruptions (incidents)
Assist in the management of incidents
Facilitate recovery from incidents
Threats
Technology R&D

FIGURE 1.1 Technology R&D in Support of Infrastructure Assurance Objectives

Both physical and cyber threats must be considered. The former include threats to tangible property produced by accidents, sabotage, and natural hazards resulting from seismic, wind and water events. The latter include electronic, radio-frequency, or computer-based attacks on the information infrastructure or its components. Other threats arise from the complexity of automated systems and from increasing interdependencies among infrastructures and between physical and cyber systems.

1.2 RESEARCH AND DEVELOPMENT ISSUE

The fundamental R&D issue for critical infrastructure protection can be framed in terms of the following three interrelated questions:

- What R&D is needed to achieve the nation's infrastructure assurance objectives?
- What level of corresponding investment is required?
- Who should make this corresponding investment?

These questions must be answered within a partnership between government and the private sector. Both entities must recognize that: (1) infrastructure assurance risks cut across the public and private sectors; (2) the private sector holds much of the relevant technical and empirical data on infrastructure operations, interdependencies and vulnerabilities; and (3) the private sector develops technology only when it identifies a market for it. Successful implementation of technologies developed from government-funded research efforts will require close cooperation with private sector owners and operators of our nation's infrastructures.

The R&D recommendations presented here do not imply that government and the private sector are not investing in protection and detection, mitigation, incident response, and recovery. Current R&D investment is inadequate, and progress is too slow to deal effectively with current and future vulnerabilities. The scale and scope of R&D investments need to be expanded to address infrastructure assurance issues from a national perspective, with a long-term view of the health and welfare of the nation.

1.3 REPORT ORGANIZATION

The remainder of this report is organized as follows. Section 2 discusses the key information sources and PCCIP-sponsored studies that provided the foundation for developing integrated R&D recommendations. Section 3 summarizes specific R&D areas and topics. Finally, Section 4 focuses on recommendations for action, including strategy and implementation recommendations, as well as investment requirements.

2. FOUNDATION FOR RECOMMENDATIONS

In developing the R&D recommendations, the PCCIP (1) drew upon recent studies (external information sources) that address problems and technology R&D needs related to critical infrastructure assurance, and (2) sponsored a series of independent studies that focused on specific R&D issues. This approach helped the PCCIP to avoid duplication; gain valuable insights into infrastructure problems from the perspective of other task forces, committees, and study panels; and identify recurring themes. Figure 2.1 highlights key information sources and PCCIP-sponsored studies that provided the foundation for developing integrated R&D recommendations. The following sections briefly describe these sources and studies.

2.1 EXTERNAL INFORMATION SOURCES

Among the many relevant studies conducted recently, eight helped the PCCIP gain perspective and formulate R&D recommendations in the key critical infrastructure area of information assurance.

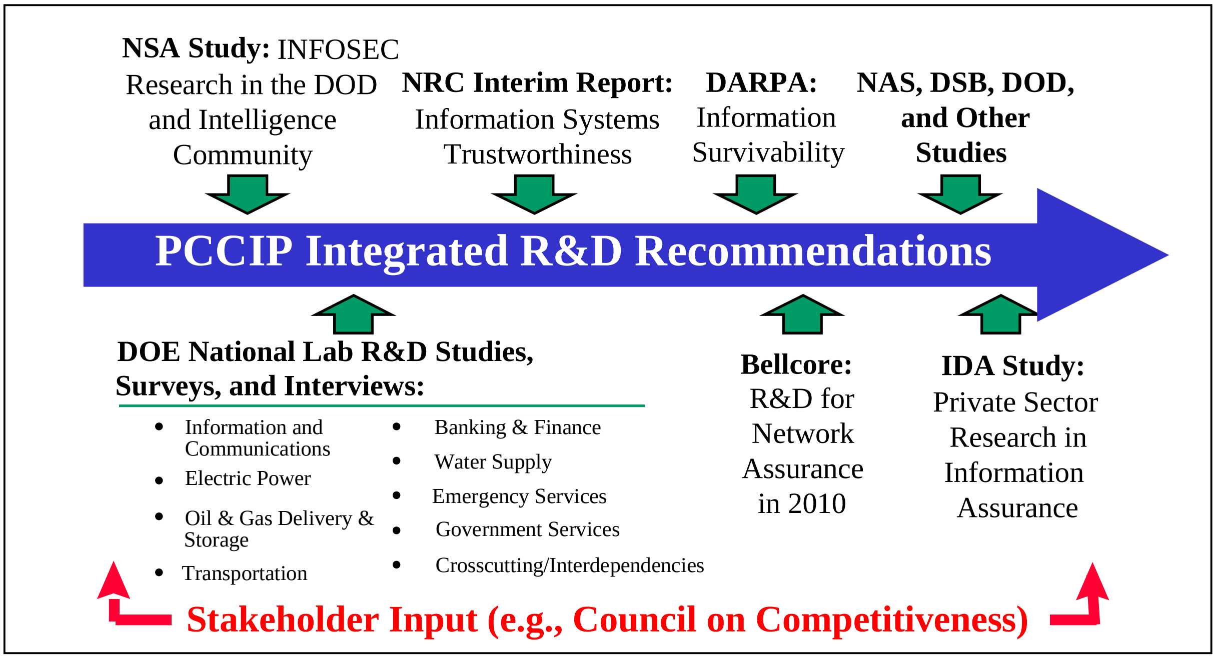
NSA Study: INFOSEC Research in the DOD and Intelligence Community
NRC Interim Report: Information Systems Trustworthiness
DARPA: Information Survivability
NAS, DSB, DOD, and Other Studies
PCCIP Integrated R&D Recommendations
DOE National Lab R&D Studies, Surveys, and Interviews:
• Information and Communications
• Electric Power
• Oil & Gas Delivery & Storage
• Transportation
• Banking & Finance
• Water Supply
• Emergency Services
• Government Services
• Crosscutting/Interdependencies
Bellcore: R&D for Network Assurance in 2010
IDA Study: Private Sector Research in Information Assurance
Stakeholder Input (e.g., Council on Competitiveness)

FIGURE 2.1 Key Sources of Information Used by the PCCIP in Developing Integrated R&D Recommendations

- ***National Research Council (NRC) Interim Report on Information Systems Trustworthiness [1]***. The motivation for the NRC report is summarized in the paragraph quoted on page 1 of this report. In particular, the NRC report elucidates a research agenda and program of technical activities for strengthening the reliability of information systems. The term “trustworthiness” encompasses all of the attributes a system must have so that society can *depend* on the system’s operation of its critical infrastructures. Potential research areas for future exploration, such as mobile code, network infrastructure, and cryptography, are identified.

- ***Defense Science Board (DSB) Report on Information Warfare - Defense [2]***. This report documents the work of a DSB Task Force that focused on protection of information interests of national importance through the establishment and maintenance of a credible information warfare defensive (IW-D) capability. The Task Force found that: (1) current security products are not designed to protect large, distributed environments; (2) the Department of Defense (DOD) must evaluate carefully emerging commercial technologies and products (e.g., examine theft and fraud versus denial of service issues); and (3) academia, industry, and government must be part of the research effort. The Task Force recommended that the IW-D R&D program focus on several key areas: including robust survivable system architectures; techniques and tools for modeling, monitoring, and managing large-scale distributed/networked systems for automating detection and analysis of localized or coordinated large-scale attacks; tools for synthesizing and projecting the anticipated performance of survivable distributed systems; and test beds and simulation-based mechanisms for evaluating emerging IW-D technology and tactics. In addition, the Task Force recommended that the R&D community should consider establishing an R&D effort focused on the theory, science, and analysis of high-assurance, massively distributed systems. To get started, the Task Force recommended an additional allocation of $580 million over the next five years (FY97–FY01) to address R&D needs in IW-D.

- ***Department of Defense Report on Improving Information Assurance [3]***. Prepared by an Information Assurance (IA) Task Force established by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, this report is a general assessment of DOD’s current IA posture. It describes a comprehensive approach for achieving an integrated IA program. The general assessment, while pointing to significant deficiencies within DOD’s IA posture, acknowledges the benefit of ongoing IA initiatives among the Defense Components and emphasizes that the DOD must maintain and build on this momentum. The report sets forth a new three-point strategy for enhancing DOD information assurance posture: (1) risk management, (2) continuous improvement, and (3) sound investments (i.e., risk reduction return on investment). Two recommendations call for a comprehensive research and technology development program that:

  - ➤ Leverages the collective capability of the Information Security (INFOSEC) research community, both public and private, and

- ➤ Ensures the availability of appropriate vulnerability countermeasures that are consistent with commercial product cycles.

- ***National Security Agency Scientific Advisory Board INFOSEC Panel [4]***. This Panel conducted a high-level examination of the INFOSEC program. In addition to advocating a stronger R&D program, the Panel made a number of recommendations, including:

  - ➤ Significantly increasing the INFOSEC R&D budget to meet the myriad of challenges that must be addressed, and

  - ➤ Developing a world class understanding of information systems and technologies, with an emphasis on network security.

- ***Joint Security Commission Report on Redefining Security [5]***. The Commission found that information systems technology is evolving much faster than information systems security technology. Therefore, a carefully planned, well-managed R&D program is required. The Commission recommended that:

  - ➤ R&D programs be given high priority in creating the secure products that DOD and the intelligence community need to protect their classified and unclassified information networks and systems, and

  - ➤ The Secretary of Defense and the Director of Central Intelligence assign NSA as the executive agent for information systems security R&D for both classified and unclassified information for DOD and the intelligence community.

- ***Report of the Commission on Protecting and Reducing Government Secrecy [6]***. The Commission noted that in the next century, the federal government and industry must work more closely to develop technologies that address the problems resulting from rapid proliferation of information systems within the government. In terms of R&D, the Commission advocated developing auditing and intrusion detection systems. Such systems must be combined with timely assessment and response capabilities to achieve effective systems security.

- ***DARPA Program on Information Survivability [7]***. The goal of this program is to provide affordable, verifiable, and scalable technologies to ensure a robust and secure defense infrastructure. The program is composed of four subareas: high-confidence computing systems, high-confidence networking, survivability of large-scale systems, and wrappers and composition. Its top three priorities are:

  - ➤ Operating system security (influence future commercial operating system development; adaptive system paradigm),

- ➤ Intrusion detection (extremely high accuracy; detection capability for unknown intrusion types), and

- ➤ Assurance technologies (well integrated into system development tools).

- ***Stanford Workshop on Protecting and Assuring Critical National Infrastructure: Setting the Research and Policy Agenda [8]***. One session focused on technologies and tools for critical infrastructure protection. In addressing the issue of who should perform research, workshop participants recommended:

  - ➤ Forming private/public partnerships to redesign the infrastructure. Sponsoring research that results in demonstration projects.

  - ➤ Funding by the government of basic research to cast the architectural framework. Challenging companies to model specific infrastructures and focus on solving problems.

2.2 PCCIP-SPONSORED STUDIES

To supplement the sources cited above, the PCCIP sponsored four external studies and one internal R&D study.

- ***National Security Agency Study on INFOSEC in the DOD and Intelligence Community [9]***. This study estimated that the government investment (including personnel costs) in INFOSEC research is approximately *$150 million per year*. The investments are weighted heavily in two areas: (1) damage avoidance, detection, and recovery; and (2) assurance. The emphasis in the former is on intrusion detection. The emphasis in assurance is on risk management. The study recommends that an additional $100–150 million per year is needed over the next three to five years to study critical INFOSEC problems.

- ***Institute for Defense Analyses (IDA) Study on Commercial Perspectives on IA R& D [10]***. The *IDA* conducted interviews with 21 computer and telecommunications technology providers to (1) assess commercial IA R&D funding and (2) determine where commercial technology providers are investing and where they think they should invest in the future.

  IDA was unable to obtain funding information from such interviews as such information is either proprietary or not uniquely captured and classified as IA research (i.e., it is integrated into product development). In the absence of such funding data, IDA independently developed a gross estimate of commercial IA R&D funding from publicly available industry data. This estimate indicates that commercial IA R&D ranges between $120 and $355 million per year. A framework for addressing IA technology R&D is provided in which the wide ranging views for IA R&D investment obtained through the interviews are organized. This framework segments the IA research needs into (1) Basic Research in IA Fundamentals, (2) System-level Security Engineering, and (3) Individual Component Development. System-level Security Engineering is the highest priority research need. The report contains the following findings:

➤ The U.S. commercial IA R&D activity is fairly robust in breadth, but is lacking in depth.

➤ Industry believes that it "owns" the commercial IA technology problem and should spend to solve it.

➤ US commercial IA R&D investment is focused on satisfying customer demand primarily in electronic commerce.

➤ All the companies interviewed indicated that their R&D investments in IA technology were increasing and that, for most companies, this trend should increase for the next few years.

➤ There are important areas of IA research that either are not being pursued by commercial technology providers or require additional emphasis and funding.

➤ Technology transfer remains a significant problem.

➤ Export control policy is perceived to be the biggest barrier to further commercial IA investment, thereby reducing the capability to protect our critical infrastructures.

➤ Government-funded research, leadership, and vision can make a difference.

- ***Department of Energy (DOE) National Laboratory R&D Studies, Survey, and Interviews [11—13]***

  ➤ Teams of subject-matter experts from the national laboratories were formed to develop technology R&D recommendations in the eight critical infrastructure areas and in the crosscutting, interdependency area. Each team examined threat and vulnerability issues, elicited stakeholder and user community inputs, analyzed trends (technology, regulatory, market, social) that impact infrastructure assurance, and reviewed commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) technologies. The teams also looked at ongoing R&D efforts that could be used to meet the identified needs. The six topical R&D categories and many of the specific recommendations in this report were based on these studies.

- ➤ A survey of the DOE national laboratories and the private sector was conducted to identify technologies and capabilities applicable to the eight critical infrastructures. More than 1,600 combinations of technologies and capabilities were identified in the vulnerability/threat assessment, detection, response, mitigation, and recovery areas that could be used to meet infrastructure assurance needs.

- ➤ More than 40 interviews, primarily with representatives of the private sector, were conducted in the eight critical infrastructure areas. Vulnerabilities, threats (physical, cyber, conventional, and unconventional), technology needs, ongoing R&D efforts, and R&D gaps were discussed. Encryption devices and techniques, network and security management, intrusion detection, physical and cyber protection technologies, and modeling and simulation tools were among the specific areas identified for continued R&D efforts.

- ***Bellcore Study on R&D for Network Assurance in 2010 [14]***. This study presents Bellcore's view and characterization of the R&D areas that are critical for providing the desired levels of network assurance in the future public telecommunications infrastructure in the United States, including both the Internet and the Public Switched Telecommunications Network. Government R&D and industry-sponsored R&D are both needed. The key recommendations of this study are that the government should maintain its current level of R&D funding and promote R&D in critical areas that directly impact network assurance. These critical R&D areas include:

  - ➤ Security (operating system security, software integrity, cryptography, intrusion detection, and firewalls);

  - ➤ Distributed control;

  - ➤ Network assurance measurement infrastructure (metrics, criteria, techniques, and tools);

  - ➤ Interprovider policy routing/architectures;

  - ➤ Advanced services (quality of service, multicast);

  - ➤ Stability of dynamic Internet Protocol and Asynchronous Transfer Mode routing protocols; and

  - ➤ New technologies, services, and applications.

  The study specifically notes that security R&D lags behind corresponding product releases and recommends continued support for critical government programs [such as the Next Generation Internet (NGI) project] that sponsor R&D in many areas that impact network assurance.

- ***Internal PCCIP Study [15]***. A detailed review of the R&D budgets of 13 major companies revealed that many R&D items that affect information security were not listed in the budgets as individual line items. The review clearly showed that many developments that would affect security were buried in other major development items. This study indicated that the private-sector R&D expenditures associated with information security range from $1 billion to $1.5 billion on an annual basis. Further, the study showed little research was being conducted in the private sector.

3. RESEARCH AREAS AND TOPICS

To address the range of physical, cyber, and other threats facing our nation's critical infrastructures, research is needed to:

- Secure information while it is stored, being processed, and in transit;
- Monitor and detect threat activity, and provide warning in real time;
- Assess the vulnerability of both components and entire infrastructures;
- Manage risk and support decision making;
- Protect infrastructures physically and mitigate damage; and
- Aid in rapid incident response and recovery.

Specific research areas and topics are identified in Table 3.1 and described in the following sections.

3.1 INFORMATION ASSURANCE

As national infrastructures increasingly depend on computers and networked information systems to improve efficiency and enhance economic competitiveness, they also become more vulnerable to potential cyber attacks. In addition, the basic technology is changing rapidly, and government policy is encouraging increased competition. These changes affect the individual critical infrastructures and national interdependent infrastructures, as well as increase infrastructure vulnerability as a whole.

Significant new investment in R&D is required to protect the communications infrastructure, and the information created, stored, processed, and transmitted on it. Security of vital information is a key component for functioning of interdependent infrastructures, such as electric power, emergency services, banking and finance, and transportation. The need to develop new means of protection is apparent, given the increasing rate of incidents, the expanding list of known vulnerabilities, and the inadequate set of solutions available. R&D recommendations for four topics in the information assurance area are discussed in the following sections.

TABLE 3.1 R&D Areas and Topics

R&D Areas	R&D Topics
Information Assurance	• System Level Security • Advanced Concepts and Theory (for Information Protection) • Management of Information Protection • Encryption Technologies
Monitoring and Threat Detection	• Automated Monitoring and Detection • Infrastructure Information System
Vulnerability Assessment and Systems Analysis	• Vulnerability Assessment Tools • Complex System Modeling • Test Beds • Verification Technologies
Risk Management and Decision Support	• Risk Management • Decision Support Systems
Protection and Mitigation	• Real-Time Distributed System Control • Infrastructure Hardening • Containment and Isolation
Incident Response and Recovery	• Response Technologies • Recovery Technologies

3.1.1 System Level Security, Engineering, and Architectures

The current and anticipated future state of the information architectures that support our national infrastructures needs to be characterized. The very nature and behavior of the system of information being exchanged among information providers and processors on the one hand, and communications channel and support providers on the other, are not well understood. Such new forms as electronic signatures, electronic money, and the virtual enterprise create new reliability and security challenges as fast as they create new economic opportunities. Understanding the anatomy and dynamics of this new system, and developing appropriate security and assurance practices, requires R&D, with the coordinated effort of government and industry.

Security architectures can be used to organize individual security components and services into working systems that provide information and resource confidentiality, integrity, and availability.

Architectures specify how protection protocols and data exchange interfaces allow the interoperation of security components. The role of architectures is becoming more important, as security services become distributed like the systems that they protect and as the software industry begins to provide individual security mechanisms as independent modules. R&D is required for addressing standards for: evaluating information protection when different tools and measures are combined in the infrastructure; characterizing architectures for robustness, scalability, and overall strength of security; streamlining performance of protective systems to reduce the costs of using them, especially in terms of time and ease of operation; and incorporating, where feasible, advanced information protection concepts, such as information that carries with it conditions for its use.

These security architectures require technologies that facilitate more efficient and effective interaction (communication) between computer-based systems and users. System complexity must be reduced, and ease of use must be enhanced without sacrificing security or increasing risk. For example, security and interactive problem-solving technologies (e.g., interactive agents), which are integral to system designs, must be developed to augment user strengths and compensate for user weaknesses.

3.1.2 Advanced Concepts and Theory (for Information Protection)

Considerable R&D is needed to provide a proper theoretical base for protecting the communications and information infrastructure and supporting different paradigms, models, and implementations. Fundamental research to generate new concepts is required on intrusion detection, malicious software, access control, authorization, authentication, interoperability, denial of service, and system complexity. Research also is needed in information protection policy development and use, reconstitution and recovery for all levels of the infrastructure, and distributed hardware and software approaches. It is assumed that research efforts associated with the NGI, which have direct implications on network assurance, will continue and provide a foundation for these research efforts. This fundamental research is critical to the establishment of a system security engineering discipline.

3.1.3 Management of Information Protection

Security management today is a major operational cost consideration. Affordable methods and techniques for the use and management of information protection methods, tools, and practices are needed to support the protection of information in the infrastructure. Improved methods are needed for remote and local configuration management of the infrastructure components. The new methods and techniques should be scaleable and must anticipate and support advanced infrastructure and networking concepts, such as active and adaptive networks.

3.1.4 Encryption Technologies

Encryption can improve information security by providing privacy and supporting data confidentiality, user identification and authentication, data integrity, and access control. Encryption also can be used for implementing message integrity, digital signatures, nonrepudiation, and advanced authentication techniques. The mathematical algorithms used to encrypt data must be highly resistant to attack and computationally secure. The keys used for encrypting and decrypting data must be distributed properly, protected, and managed. Promising new encryption technologies, such as elliptic curve, could improve both security and economy of operations. New concepts of key management infrastructure could emerge to provide a variety of alternatives that industry could develop into interoperable products.

3.2 MONITORING AND THREAT DETECTION

Reliable automated monitoring and detection systems, timely and effective information collection technologies (e.g., using intelligence, open source, and voluntarily contributed private-sector information), and efficient data reduction and analysis tools are needed for identifying and characterizing localized or coordinated large-scale attacks against critical infrastructures. A “civil defense” capability in the cyber environment (National Cyber Defense) is an appropriate consideration to provide a national perimeter defense resulting in “defense in depth” protection and attack sensing and warning. In addition to supporting protection of the individual elements of the critical infrastructure, such a concept could facilitate communication of threat situations between and among these elements. It could also facilitate the exchange of technical information and technologies needed to ensure adequate protection at the element level. Such technologies would support early threat warning to government organizations and private-sector infrastructure owners and operators, thereby preventing widespread infrastructure disruptions that have potentially serious consequences on our national security, economy, and quality of life. As described below, both hardware (monitoring and detection devices) and software R&D activities are needed.

3.2.1 Automated Monitoring and Detection

Technologies that automatically monitor infrastructure and detect intrusions are crucial for establishing a more proactive approach to infrastructure assurance. Research is needed for developing monitoring technologies for sensing system instabilities and voltage collapse in the electric power sector, highly sensitive biological and chemical agent detectors for real-time monitoring of public spaces and water supply systems, automated technologies for detecting electronic intrusions into infrastructure control systems (e.g., supervisory control and data acquisition [SCADA] systems), and advanced terminals and real-time vehicle and cargo monitoring technologies. Advanced infrastructure monitoring techniques also are needed to detect dangerously deteriorating conditions in structures (e.g., “smart” sensors and “smart” materials technology, such as ultrasonic or magnetic corrosion detection, embedded fiber optics for enhanced visual inspection, and shape-memory alloys). Monitoring stations, similar to those in use by the electric power industry, are needed for other infrastructures.

3.2.2 Infrastructure Information System

The ability to prevent, mitigate, respond to, and recover from an attack could be enhanced significantly by developing and using advanced geographic information systems (GISs). These systems use remote sensing and geographic positioning system (GPS) technologies. While information exists for some infrastructures (e.g., gas and oil pipelines), it is not comprehensive and integrated. The collection of intelligence and other information (e.g., monitoring data) is the critical first step in identifying and characterizing threats, supporting policy-making and investment decisions, and providing timely, effective indications and warning systems. Threat assessment, threat warning, attack alert, and attack assessment concepts, tools, systems, and processes—as well as mitigation, incident management, and recovery systems—all directly depend on the timeliness and accuracy of information. "One-call" centers for real-time information about the location of critical infrastructure components, which would speed responses to threats and disasters, are possible only if accurate "as built" plans are available and highly detailed GIS/GPS technologies are developed.

Technologies and a process are needed to pull together sharable, appropriately sanitized information from the intelligence community, the law enforcement community, and the private sector to understand the dimension of potential threats. The information conveying the balance of threats and vulnerabilities needs to be plausible to warrant the investment of limited resources in assurance. Classified and proprietary informational issues must be addressed so that information sharing between government and industry is improved without compromising competitive advantage or shaking the confidence of customers and investors.

On-line and automated data reduction and analysis tools are an integral part of an information system for early detection and characterization of threats (physical or cyber) to one or more infrastructures. Timely data reduction and analyses provide vital information for assessing the extent of damage and the necessary information to simulate potential propagation through the infrastructures. Such information could help to select efficient response and recovery strategies. Timely automated data analyses techniques (e.g., time series analyses, pattern recognition, regression) on large sets of data, including data from real-time monitoring and detection systems, require innovative R&D efforts because of their complexity.

3.3 VULNERABILITY ASSESSMENT AND SYSTEMS ANALYSIS

Advanced methods and tools for assessing vulnerability and analyzing systems are needed to identify critical nodes within infrastructures, to examine infrastructure interdependencies, and to help understand the behavior of complex systems. These methods and tools would help address physical and cyber security issues in an integrated fashion. Modeling and simulation tools and environments (e.g., test beds) for studying infrastructure-related problems also are important.

The advantage of modeling is that it allows experimentation that cannot be performed in realistic environments of any appreciable scale. Techniques also are needed to verify and validate methodologies and tools used for designing and building new systems, and to assess existing systems.

3.3.1 Vulnerability Assessment Tools

Vulnerability assessment tools are needed to determine the specific exploitable weaknesses (vulnerabilities) of infrastructure systems and components to credible threats. An example is vulnerabilities in administrative controls for operating and managing computer systems. Tools are needed to: measure the relative risks in terms of probability of occurrence, likelihood of success, and the degree of impact on national security, economic competitiveness, quality of life, and other important attributes; and to identify critical nodes and components where propagation could exacerbate the impact. These tools are necessary: to support national and local planning, prioritization, decision making, and investment strategies; to enhance the ability of users to perform consequence assessment and risk analysis; and to develop effective risk management approaches and strategies. In addition, technology assessments are required so that the infrastructure protection community can develop a comprehensive awareness of: (1) the inherent susceptibilities of current and future technologies on which infrastructures and key components are or will be reliant; (2) technologies that potentially could be used maliciously to disrupt, damage, or destroy infrastructures or key components; and (3) technologies that could have protective applications and potential for safeguarding infrastructures and components.

3.3.2 Complex System Modeling

In-depth research on the complexities and interdependencies in the critical infrastructures is needed. While "complexity" research has continued at an abstract level, the complexity/interdependency problem, as it relates to practical infrastructure assurance, has not been studied in depth. This research would provide the empirical and theoretical foundation for developing a diverse vulnerability assessment, monitoring, predictive modeling, and consequence analysis technologies needed for addressing infrastructure assurance issues.

Robust infrastructure and nodal analysis techniques and tools need to be developed for modeling large-scale distributed/networked systems and interdependent infrastructures. Such tools would facilitate identifying critical infrastructure nodes and components, the interdependencies among infrastructures, and the consequences resulting from degradation or loss of infrastructure capabilities. Advanced tools and methods also are required to support the identification and mapping (physically and logically) of infrastructure systems, the location of critical nodes and components, and the identification and quantification of net consequences to users (government and the private sector) in the event of degradation or loss. Such tools and methods also are needed to help assess the required redundancy margins and firebreaks to preclude catastrophic failures.

3.3.3 Test Beds

National, regional, and virtual test beds are needed (1) to test the nation's infrastructure under actual working conditions and (2) to test analysis, assessment, advanced predictive modeling, and other modeling and simulation systems and tools. Test beds allow scientists to perform experiments on different infrastructures and components, investigate incidents, examine improvements to hardware and software, examine genetic diversity issues, and conduct other necessary experiments usually too expensive and/or disruptive to be performed otherwise. The Next Generation Internet (NGI) could be an appropriate vehicle for large-scale experimentation and development into a new highly assured Internet backbone.

3.3.4 Verification Technologies

Substantial research has gone into formal methods to design and develop systems that can be proven to meet their design requirements. However, hardware and software bugs continue to be introduced. There is an urgent need for research on total design and verification strategies that can be applied to subsystems and the composition of subsystem of the critical infrastructure. While the entire problem may not be tractable, there may be subsets that are. It is vital to understand what is possible and then to fund research that will lead to high reliability systems. Automated technologies need to be developed, for example, that can uncover hidden “logic bombs” in critical software systems and, with a high level of confidence, the veracity and validity of software systems. In addition, more work needs to be done on hardware verifications.

3.4 RISK MANAGEMENT AND DECISION SUPPORT

Risk management and decision support system methodologies and tools are needed to help government and private-sector decision makers to prioritize the use of limited resources to reduce risk. These methodologies and tools would address risk both from familiar threats (e.g., natural disasters, physical attack) and from emerging and future threats, such as risk from our increasing interdependence and reliance on cyber systems.

3.4.1 Risk Management

Methodologies, tools, and organization processes are needed to identify and minimize the impact of risks on infrastructure sectors and information. Research areas include developing methodologies: for formulating management decisions based on operational missions and information value; for dealing with uncertainties in, or incomplete knowledge of, threats, vulnerabilities, and protection measures; and for managing risks across the multiple components and organizations involved in the infrastructures.

It is essential to understand the consequences of disruptions to our infrastructures to make effective decisions. A set of comprehensive analytical tools is needed to facilitate predictive rapid and detailed “post-mortem” analyses of disruptions that affect single or multiple infrastructures. These tools would facilitate investigation and estimation of the consequences of the disruption at the national, regional, and local levels. The tools would address in a systematic and comprehensive way, for example, economic impacts (direct and indirect), health and safety impacts, environmental impacts, and socioeconomic impacts.

3.4.2 Decision Support Systems

Decision analysis (which encompasses cost-benefit analysis) tools are needed for prioritization, facility siting, and resource allocation decisions. For example, these tools help identify and prioritize critical assets for protection and restoration, compute return on investment in competing security technologies, and develop overall infrastructure investment strategies. Measurable criteria need to be established that address national security, economic competitiveness, quality of life, and other important attributes, such as capital, operation and maintenance, and life-cycle costs. In the information and communications sector, methodologies and tools are needed to assist information owners in determining what protection is appropriate for information and in understanding the value or costs of information. This knowledge will enable them to judge what, where, and how much protection is needed. Such methodologies would help determine what infrastructure assets are critical and thus aid in the priority use of resources in a degraded environment.

Formalized techniques/tools are needed for predicting, testing, and verifying complex system performance. These tools help predict the behavior and properties of large-scale, complex systems that involve one or more infrastructures and infrastructure dependencies. They also are needed to help support decisions on how these systems can be protected/isolated and degraded gracefully, if necessary, to prevent cascading impacts. Research on behavior properties, parameter estimation, advanced artificial intelligence, and other innovative techniques will be required.

Lessons learned systems need to be developed to provide planners and analysts with a quick reference to past disruptions/events, initiating causes, impacts and consequences, corrective/protective, legal, and legislative/regulatory actions taken, organizational roles and responsibilities, and other key information. Lessons learned can be supplemented through exercises and simulations. Such information would be invaluable in supporting both proactive and reactive decisions to disruptions. A comprehensive up-to-date interactive distributed knowledge base (encyclopedia) of protection technologies and countermeasure techniques also would be helpful in ensuring that planners and operators are aware of the full range of protection options. This encyclopedia could address associated factors, such as cost, practicality, effectiveness, operational penalties, and maturity, which normally are used in making decisions.

3.5 PROTECTION AND MITIGATION

Real-time system control, infrastructure hardening, and containment and isolation technologies also are needed to protect infrastructure systems against the entire threat spectrum. Other current and advanced survivability, reliability, or assurance enhancement measures need to be explored and developed. Three aggregated research topics are described in the following sections.

3.5.1 Real-Time Distributed System Control

Real-time distributed system control technologies are needed to help protect and improve the efficiency and effectiveness of existing infrastructures. These technologies would reduce the need to build costly new infrastructures that may pose environmental, regulatory, and other undesirable problems. For example, the advanced real-time control technologies for electric power systems would allow better use of transmission and distribution systems.

3.5.2 Infrastructure Hardening

R&D work needs to enhance the ability of various infrastructures to survive disruptions of larger magnitude than previously considered. Guidance can be provided by the efforts of industry and government to engineer greater seismic margins into buildings located in earthquake-prone zones. Both physical and cyber systems need to be considered.

3.5.3 Containment and Isolation

Impact containment and isolation technologies are needed that limit the amount of damage due to chemical or biological contamination, explosions, information system disruption or data contamination, and other acts of terrorism. For example, blast-resistant containers are needed to reduce the impacts of explosive devices placed in vehicles or cargo holding facilities. Technologies that contain and isolate chemical and biological contaminants released in air and water supplies are needed to minimize exposure to the population. Technologies also are needed to contain and isolate the impacts of information system disruptions so that neither the complete system or interdependent infrastructures are affected.

3.6 INCIDENT RESPONSE AND RECOVERY

A wide range of new technologies and tools are needed for planning for, responding to, and recovering from incidents, such as natural disasters and physical and cyber-based attacks, that affect local or national infrastructures. Advanced planning methods and tools supporting preparation for, mitigation of, response to, and recovery from infrastructure attacks or failures are desired. R&D needs are described below.

3.6.1 Response Technologies

Technologies are needed that can aid in responding to a disruption of infrastructure. Tools are needed: for quick assessment of the size and location of populations at risk (e.g., from a chemical or biological agent) and the location of structures under imminent threat of damage; for optimal selection, dispatch, and routing of medical, police, fire, and other responders; and for crisis and consequence management that identify the infrastructure owners and operators, and the roles, responsibilities, authorities, and capabilities of federal, state, and local response organizations. For example, technologies are needed to speed the delivery or re-establishment of transportation services for an affected area, and to improve protective equipment and communications capabilities for emergency responders.

3.6.2 Recovery Technologies

Technologies need to be developed to aid in the rapid recovery and restoration of infrastructure and infrastructure-related services. This broad R&D area ranges from emergency medical and decontamination technologies to respond to, and recover from, a chemical or biological agent attack involving contamination of a municipal water supply, a major metropolitan area, or a federal facility, to technologies to recover from a highly destructive cyber assault on the stock exchanges and banking systems. Advanced technologies are needed to support federal, state, and local response organizations.

4. RECOMMENDATIONS FOR ACTION

A joint R&D effort among government, industry, and academia is needed to produce a successful infrastructure assurance research and technology development effort. The strategy and implementation recommendations presented in this section are made assuming a joint effort, and recognizing that R&D is only one component of an overall national infrastructure assurance strategy.

4.1 STRATEGY AND IMPLEMENTATION RECOMMENDATIONS

- *A focal point (coordinating entity) for national infrastructure assurance R&D efforts should be established.* Figure 4.1 illustrates this concept. This entity, which may be a successor to the PCCIP, would stress partnership between government and the private sector, coordinate with established advisory and information exchange groups, and promote awareness and education. Its missions would include developing, coordinating, prioritizing, and overseeing the R&D agenda to meet critical national needs. It also would serve as a clearinghouse for disseminating such information.

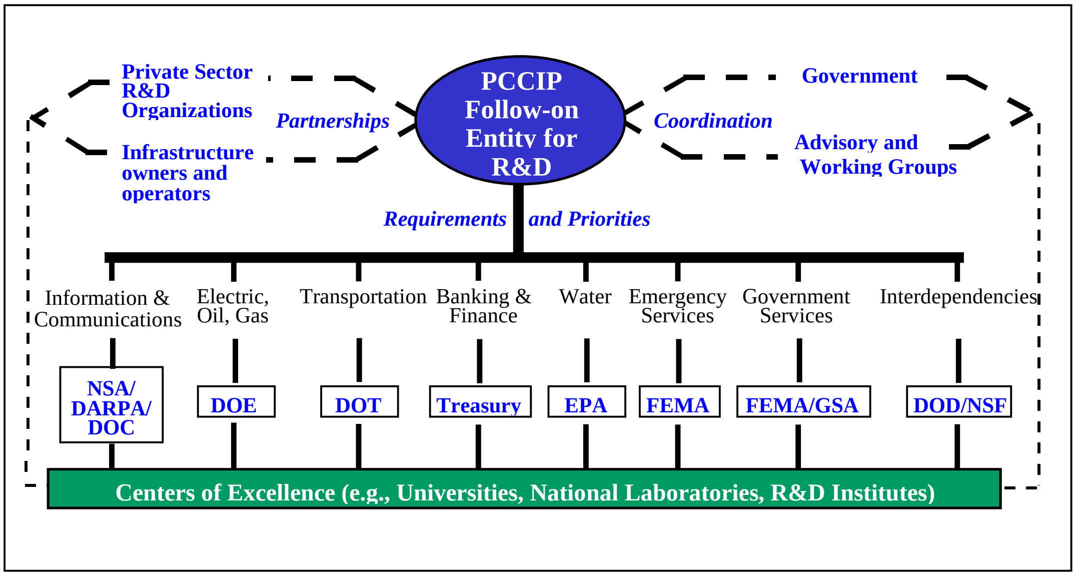
Private Sector R&D Organizations
Infrastructure owners and operators
Partnerships
PCCIP Follow-on Entity for R&D
Coordination
Government
Advisory and Working Groups
Requirements
and Priorities
Information & Communications
Electric, Oil, Gas
Transportation
Banking & Finance
Water
Emergency Services
Government Services
Interdependencies
NSA/ DARPA/ DOC
DOE
DOT
Treasury
EPA
FEMA
FEMA/GSA
DOD/NSF
Centers of Excellence (e.g., Universities, National Laboratories, R&D Institutes)

FIGURE 4.1 Infrastructure Assurance R&D Organizational Structure

- *Appropriate lead agencies should manage infrastructure-specific R&D efforts.* Close coordination with federal entities and with established advisory and information exchange groups is essential to ensure efficient use of limited funds. Partnerships must be established with private-sector R&D organizations and infrastructure owners and operators, and centers of excellence must be identified/established at universities, national laboratories, and private-sector R&D institutes. The responsible lead agencies should set their specific R&D agendas on the basis of established national objectives and guidance provided by a coordinating entity.

- *The National Research Council (NRC) should define more fully a national infrastructure assurance research program based on the information contained in this report.* The NRC should lead the effort, together with those departments and agencies of the federal government already engaged in R&D relevant to each infrastructure.

- *Promote the discipline of complex, interdependent systems engineering.* This discipline would provide the theoretical foundation for developing the diverse vulnerability assessment, monitoring, predictive modeling, and consequence analysis technologies needed for addressing infrastructure assurance issues as they relate to the eight critical infrastructures. Concepts, such as system complexity, interaction, and coupling, would be examined. This new discipline is fundamental in providing large-scale system engineering and high confidence systems.

- *In-depth research on the complexities and interdependencies in the national infrastructures is needed.* While research is ongoing in many topical areas (e.g., modeling the power grid), the interdependency problem has not been studied in depth. Research that evaluates actual incidents and probes possible scenarios would lead to a more focused research agenda.

- *A national repository of validated infrastructure-related models and data (including GIS information) should be established and linked closely to the test beds.* The test beds would be used to test the nation's infrastructure under actual working conditions, and test analysis, assessment, advanced predictive modeling, and other modeling and simulation systems and tools. Such a repository would support prevention, mitigation, incident response, and recovery objectives in both planning and analysis and crisis situations.

- *Various forums, such as conferences, workshops, and government and private-sector planning meetings, should be established.* These forums would bring together researchers, private-sector infrastructure owners and operators, and government to discuss common problems and requirements, to establish research agenda, and to promote creative thinking on solutions to infrastructure problems.

- *Training, education, and awareness programs should be established.* First, these programs would develop a cadre of knowledgeable people ("infrastructure practitioners"). Second, they would ensure proper implementation and utilization of new technologies, methods, and tools.

4.2 INVESTMENT REQUIREMENTS

It is estimated that the government needs to invest approximately $500 million to $1 billion per year to address the infrastructure assurance R&D areas and topics identified in Table 3.1. A recommended investment profile for FY98 through FY04 is shown in Table 4.1. Information assurance is a separate item because it represents the largest single area needing R&D investment.

TABLE 4.1 Recommended Government Infrastructure Assurance R&D Investments

	Investment ($ Millions)						
R&D Investment Category	**FY98**	**FY99**	**FY00**	**FY01**	**FY02**	**FY03**	**FY04**
Information Assurance	150	300	360	420	480	540	600
Other Areas of Infrastructure Assurance	100	200	240	280	320	360	400
Total	250	500	600	700	800	900	1,000

To put these requirements into perspective, the recommended investment of $500 million in FY99 represents an approximate doubling of the current infrastructure assurance R&D funding level.[2] This increase in investment is needed to "jump start" a focused, coordinated, and goal-oriented national R&D effort. As shown in Table 4.1, the recommended level of investment would double again over the next five-year period (FY00–FY04), as the R&D program gains momentum and achieves critical mass in terms of researchers and innovative research ideas.

[2] As noted in Section 2.2, the current government investment in INFOSEC research (information assurance) is approximately $150 million per year. R&D investments in the other infrastructure assurance areas are more difficult to quantify because much of the relevant work is not identified explicitly or reported as being related to infrastructure assurance. Further, considerable value judgment must be applied in determining what specific R&D work should be so designated. Most research is likely to have been initiated for other purposes but is nevertheless applicable to infrastructure assurance needs. Overall, it is estimated that information assurance R&D needs constitute approximately 60% or more of the total infrastructure assurance R&D needs. This ratio is reflected in the recommended R&D investment profile shown in Table 4.1.

A similar or greater level of commitment and R&D investment is needed from the private sector. However, more comprehensive and detailed examinations are needed in the following areas: (1) specific R&D needs, (2) commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) technologies that could be adapted to meet those needs, (3) ongoing R&D that could be leveraged, (4) legacy systems, (5) development timeframes, (6) development dependencies, and (7) potential implementation strategies (e.g., involving government laboratories, the private sector, and academia). Once these examinations have been completed, a final national technology R&D agenda and investment strategy for infrastructure assurance can be established.

5. REFERENCES

1. *NRC, Information Systems Trustworthiness Interim Report*, prepared by National Research Council Computer Science and Telecommunications Board, published by National Academy Press, Washington, D.C. (1997).

2. DOD, *Information Warfare - Defense (IW-D)*, U.S. Department of Defense, Office of the Undersecretary of Defense for Acquisition & Technology, Defense Science Board Task Force, Washington, D.C. (Nov. 1996).

3. DOD, *Improving Information Assurance (IA): A General Assessment and Comprehensive Approach to an Integrated IA Program for the Department of Defense*, U.S. Department of Defense, Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Information Assurance Task Force, Washington, D.C. (Mar. 28, 1997).

4. National Security Agency, report prepared by the Scientific Advisory Board INFOSEC Panel (1997).

5. Joint Security Commission, *Redefining Security*, report to the Secretary of Defense and Director of Central Intelligence, Washington, D.C. (Feb. 28, 1994).

6. *Report of the Commission on Protecting and Reducing Government Secrecy*, U.S. Senate, Document 105-2, Washington, D.C. (1997).

7. Lunt, T., *DARPA Program on Information Survivability*, presentation (Aug. 1997).

8. Bambos, N., “Technologies & Tools for Critical Infrastructure Protection: Summary of Tools Session,” presented at *Workshop on Protecting and Assuring Critical National Infrastructure: Setting the Research and Policy Agenda*, Stanford University, Calif. (July 21–22, 1997).

9. Burnham, B., INFOSEC *Research in the DOD and Intelligence Community*, Private Communications (July 1997).

10. Mayfield, W., and R. Ross, *Evolving a National Information Assurance Research Agenda: Issues and Opinions from Commercial Information Technology Providers*, report prepared for the President’s Commission on Critical Infrastructure Protection by Institute for Defense Analyses, Alexandria, Va. (July 1997).

11. DOE, *Technology Research and Development Recommendations for Protecting and Assuring Critical National Infrastructures*, report prepared for the President's Commission on Critical Infrastructure Protection by U.S. Department of Energy National Laboratory R&D Teams (July 1997).

12. ANL, *National Laboratory and Private Sector Technologies and Capabilities for Protecting Critical Infrastructures*, report prepared for the President's Commission on Critical Infrastructure Protection by Argonne National Laboratory, Argonne, Ill. (July 1997).

13. ANL, *Summary Report on Critical Infrastructure Interviews*, report prepared for the President's Commission on Critical Infrastructure Protection by Argonne National Laboratory, Argonne, Ill. (July 1997).

14. Bellcore, *Research and Development for Network Assurance in 2010*, report prepared for the President's Commission on Critical Infrastructure Protection by Bellcore, Morristown, N.J. (July 25, 1997).

15. Adams, M., Private Communication (Sept. 1997).